

ABSTRACT

An authentication system in which unauthorized acquisition of the private information by a third party in the course of authentication of a user by a service provider is rendered difficult. In an authentication system in which a card 10 and a host computer 20 are interconnected over a connection line 30, the card 10 includes a memory for ID 11 for storing the card ID, an input unit 12 fed with a secret identification number, a card side interface 13 connected to the host computer 20, an information encryption unit 14 for generating the information for authentication by mixing a random number, sent from the host computer 20 and having a unique value each time it is sent, with the secret identification number of the card, and by encoding the resulting mixed signal, and a transient storage unit 15 for transiently storing the information for authentication as obtained by the information encryption unit 14.